UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,564	10/10/2003	Keith Woodard	PED-001	9439

21323 7590 01/09/2006

TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110

EXAMINER	
BAYARD, DJENANE M	
ART UNIT	**PAPER NUMBER**
2141	

DATE MAILED: 01/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/683,564	WOODARD ET AL.	
	Examiner	Art Unit	
	Djenane M. Bayard	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-4, 9-15, 19-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2004/0264435 to Chari et al as in view of U.S. Patent Application No. 2004/0268145 to Watkins et al.

a. As per claim 1, 15 and 26, Chari et al teaches a method for scanning network devices connected to a network, comprising: (a) detecting connection of a first network device to the network (See page 3, paragraph [0058], *detecting the client includes detecting a Mac address of the client, and determining an IP address of the client, when a client device is attached to an access network, the Mac address of the client device can be detected*). However, Chari et al fails to teach scanning of the first network device in response to detection of the first network device.

Watkins et al teaches wherein the gateway either routes the user directly to the sign on page or determines that the user's remote network device should be scanned for security integrity (See page 3, paragraph [0046-0047])

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate scanning of the first network device in response to detection of the first network device as taught by Watkins et al in the claimed invention of Chari et al in order to provide for a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

b. As per claim 2, Chari et al in view of Watkins et al teaches the claimed invention as described above. Furthermore, Chari et al teaches wherein step (a) further comprises inspecting data packets communicated over the network (See page 3, paragraph [0058]).

c. As per claims 3 and 16, Chari et al in view of Watkins et al teaches the claimed invention as described above. Furthermore, Chari et al teaches wherein the detecting step further comprises querying a database (See page 4, paragraph [0072]).

d. As per claim 4, Chari et al in view of Watkins et al teaches the claimed invention as described above. Furthermore, Chari et al teaches broadcasting pings on the network, continuously examining address resolution protocol tables, continuously monitoring event logs, transmitting a Lightweight Directory Access Protocol (LDAP) query, and transmitting a Domain Name System query (See page 4, paragraph [0061]).

e. As per claim 9, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach scanning at least one of a configuration, file, data, a software version, a patch, inventory, hardware, and a security vulnerability of the first network device.

Watkins et al teaches scanning at least one of a configuration, file, data, a software version, a patch, inventory, hardware, and a security vulnerability of the first network device (See page 3, paragraph [0047], *reading files, reading directories, running programs... etc*)

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate scanning at least one of a configuration, file, data, a software version, a patch, inventory, hardware, and a security vulnerability of the first network device as taught by Watkins et al in the claimed invention of Chari et al in order to provide for a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

f. As per claim 10, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach wherein step (b) further comprises updating at least one of a configuration, file, data, a software version, inventory, and a security vulnerability of the first network device.

Watkins et al teaches updating at least one of a configuration, file, data, a software version, inventory, and a security vulnerability of the first network device (See page 3, paragraph [0047]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate updating at least one of a configuration, file, data, a software version, inventory, and a security vulnerability of the first network device as taught by Watkins et al in the claimed invention of Chari et al in order to provide a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

g. As per claim 11, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach wherein step (b) further comprises comparing at least one security setting of the first network device with a predetermined security setting.

Watkins et al teaches comparing at least one security setting of the first network device with a predetermined security setting (See page 1, paragraph [0009]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate comparing at least one security setting of the first network device with a predetermined security setting as taught by Watkins et al in the claimed invention of Chari et al in order to determine if a remote device does or does not conform to a defined best practices configuration of the network (See page 1, paragraph [0009]).

h. As per claim 12, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach wherein step (b) further comprises at least

one of installing a software patch on the first network device, installing anti-virus software on the first network device, and determining if the first network device is part of a windows domain.

Watkins et al teaches at least one of installing a software patch on the first network device, installing anti-virus software on the first network device, and determining if the first network device is part of a windows domain (See Page 3, paragraphs [0046-0047]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein step (b) further comprises at least one of installing a software patch on the first network device, installing anti-virus software on the first network device, and determining if the first network device is part of a windows domain as taught by Watkins et al in the claimed invention of Chari et al in order to provide a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

i. As per claims 13, 19 and 25, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach at least one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first network device based on results of the scan, and quarantining the first network device.

Watkins et al teaches one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first 1, paragraph [0009], *the results of these checks are returned via the web and are used for security decisions involving the granting of authorization to access network services*).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate at least one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first network device based on results of the scan, and quarantining the first network device as taught by Watkins et al in the claimed invention of Chari et al in order to provide a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

j. As per claims 14 and 20, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results.

Watkins et al teaches at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results (See page 1, paragraph [0009]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results as taught by Watkins et al in the claimed invention of Chari et al in order a reliable client integrity scheme that can consistently regulate

access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

k. As per claim 21, Chari et al teaches a method for examining a first network device connected to a network, comprising: (a) querying a database for data representing connection of network devices to a network (See page 4, paragraph [0060]); (b) determining connection of a first network device to the network by locating data about the first network device in the database (See page 4, paragraph [0060]; (c) determining properties associated with the first network device to determine the identity of the first network device (See page 3, paragraph [0058]0; However Chari et al fails to teach (d) determining items to scan based on at least one of the properties; and (e) performing remote scanning of the first network device in response to the determination of the connection of the first network device to the network.

Watkins et al teaches wherein the gateway either routes the user directly to the sign on page or determines that the user's remote network device should be scanned for security integrity (See page 3, paragraph [0046-0047])

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate scanning of the first network device in response to detection of the first network device as taught by Watkins et al in the claimed invention of Chari et al in order to provide for a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

l. As per claim 22, Chari et al in view of Watkins et al teaches the claimed invention as described above. Furthermore, Chari et al teaches wherein step (c) further comprises determining at least one of credentials associated with the first network device and type of the first network device (See page 4, paragraph [0059-0061]).

m. As per claim 23, Chari et al in view of Watkins et al teaches the claimed invention as described above. Furthermore, Chari et al teaches wherein step (c) further comprises at least one of querying a database where the identity has already been determined, examining network traffic, analyzing network behavior, probing the device for signature responses, and logging into the device to query data (See page 4, paragraph [0060]).

n. As per claim 24, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach wherein step (e) further comprises selecting a set of security policy settings to audit.

Watkins et al et al teaches selecting a set of security policy settings to audit (See page 1, paragraph [0009]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate selecting a set of security policy settings to audit as taught by Watkins et al in the claimed invention of Chari et al in order to provide for a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

3. Claims 5-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2004/0264435 to Chari et al as in view of U.S. Patent Application No. 2004/0268145 to Watkins et al as applied to claim 1 above, and further in view of U.S. Patent Application No. 2001/0047401 to Moore et al.

a. As per claim 5, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al in view of Watkins et al fails to teach wherein step (b) further comprises determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network.

Moore et al teaches a system and methods for determining the physical location of a computer's network interface. Furthermore, Moore et al teaches determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network (See page 9, paragraph [0111]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network as taught by Moore et al in the claimed invention of Chari et al in view of Watkins et al in order to determine the connectivity type of the networks (See page 9, paragraph [0112]

b. As per claim 6, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al in view of Watkins et al fails to teach wherein step (b) further comprises determining a property of the first network device.

Moore et al teaches wherein step (b) further comprises determining a property of the first network device (See page 9, paragraph [0111]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein step (b) further comprises determining a property of the first network device as taught by Moore et al in the claimed invention of Chari et al in view of Watkins et al in order to determine the connectivity type of the networks (See page 9, paragraph [0112]).

c. As per claim 7, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al in view of Watkins et al fails to teach wherein step (b) further comprises determining identity of the first network device.

Moore et al teaches wherein step (b) further comprises determining identity of the first network device (See page 9, paragraph [0111]).

It would have bee obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein step (b) further comprises determining identity of the first network device as taught by Moore et al in the claimed invention of Chari et al in view of Watkins et al in order to determine the connectivity type of the networks (See page 9, paragraph [0112]).

d. As per claim 8, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al fails to teach wherein the determining of the identity of the first network device further comprises at least one of querying a database where the type has been determined, examining network traffic, analyzing network behavior, probing the first network device for signature responses, attempting to log into the device using a series of protocols, logging into the first network device and querying data within the device.

Watkins et al teaches wherein the determining of the identity of the first network device further comprises at least one of querying a database where the type has been determined, examining network traffic, analyzing network behavior, probing the first network device for signature responses, attempting to log into the device using a series of protocols, logging into the first network device and querying data within the device (See page 3, paragraphs [0046-0049]). It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the determining of the identity of the first network device further comprises at least one of querying a database where the type has been determined, examining network traffic, analyzing network behavior, probing the first network device for signature responses, attempting to log into the device using a series of protocols, logging into the first network device and querying data within the device as taught by Watkins et al in the claimed invention of Chari et al in order to provide for a reliable client integrity scheme that can consistently regulate access to network services or resources on the observed integrity properties of remote network devices requesting access (See page 1, paragraph [0007]).

4. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2004/0264435 to Chari et al as in view of U.S. Patent Application No. 2004/0268145 to Watkins et al as applied to claim15 above, and further in view of U.S. Patent No. 6,324656 to Gleichauf et al.

a. As per claim 16, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al in view of Watkins et al fails to teach wherein the detecting module continuously polls a database for data corresponding to newly attached network devices.

Gleichauf et al teaches wherein the detecting module continuously polls a database for data corresponding to newly attached network devices (See col. 4, lines 20-40).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the detecting module continuously polls a database for data corresponding to newly attached network devices as taught by Gleichauf et al in the claimed invention of Chari et al in view of Watkins et al in order to perform analysis on the entries in the database by comparing the entries with a rule set to determine potential vulnerabilities (See col. 2, lines10-15)

b. As per claim 17, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al in view of Watkins et al fails to teach fails to teach

wherein the scanning module remotely scans the first network device upon detecting data corresponding to the first network device in the database.

Gleichauf et al teaches remotely scanning the first network device upon detecting data corresponding to the first network device in the database (See col. 4, lines 20-40).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate remotely scans the first network device upon detecting data corresponding to the first network device in the database as taught by Gleichauf et al in the claimed invention of Chari et al in view of Watkins et al in order to perform analysis on the entries in the database by comparing the entries with a rule set to determine potential vulnerabilities (See col. 2, lines10-15)

c. As per claim 18, Chari et al in view of Watkins et al teaches the claimed invention as described above. However, Chari et al in view of Watkins et al fails to teach fails to teach a history database storing scan results of a scan performed by the scanning module.

Gleichauf et al teaches a history database storing scan results of a scan performed by the scanning module (See col. 2, lines 10-15).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate a history database storing scan results of a scan performed by the scanning module as taught by as taught by Gleichauf et al in the claimed invention of Chari et al in view of Watkins et al in order to perform analysis on the entries in the database by comparing the entries with a rule set to determine potential vulnerabilities (See col. 2, lines10-15).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Djenane M. Bayard whose telephone number is (571) 272-3878. The examiner can normally be reached on Monday- Friday 5:30 AM- 3:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Djenane Bayard

Patent Examiner

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER